

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2005-513913

(P2005-513913A)

(43) 公表日 平成17年5月12日(2005.5.12)

(51) Int.Cl.⁷

H04L 9/08

F I

H04L 9/00

G01D

H04L 9/00

G01E

テーマコード(参考)

5J104

審査請求 未請求 予備審査請求 未請求 (全 28 頁)

(21) 出願番号 特願2003-555730 (P2003-555730)
 (86) (22) 出願日 平成14年12月5日(2002.12.5)
 (85) 翻訳文提出日 平成16年6月11日(2004.6.11)
 (86) 国際出願番号 PCT/JP2002/012738
 (87) 国際公開番号 W02003/055132
 (87) 国際公開日 平成15年7月3日(2003.7.3)
 (31) 優先権主張番号 特願2001-389452 (P2001-389452)
 (32) 優先日 平成13年12月21日(2001.12.21)
 (33) 優先権主張国 日本国(JP)
 (81) 指定国 EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), AU, CN, JP, KR

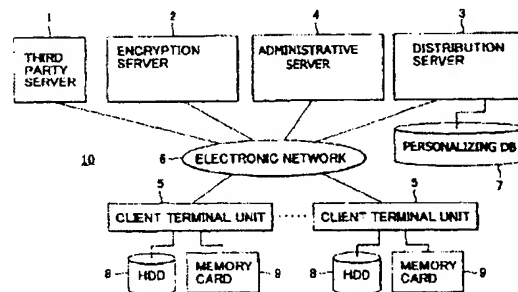
(71) 出願人 395015319
 株式会社ソニー・コンピュータエンタテインメント
 東京都港区南青山二丁目6番21号
 (74) 代理人 100099324
 弁理士 鈴木 正剛
 (74) 代理人 100108604
 弁理士 村松 義人
 (74) 代理人 100111615
 弁理士 佐野 良太
 (72) 発明者 島田 宗毅
 日本国東京都港区南青山2-6-21 株式会社ソニー・コンピュータエンタテインメント内

最終頁に続く

(54) 【発明の名称】 プログラムのセキュアな配布方法及び装置

(57) 【要約】

【課題】本発明に従った方法及び装置は、処理装置で暗号化されたプログラムを受信する過程と、ネットワークを通じて管理装置に機器IDを伝送する過程、機器IDに回答して、ネットワークを通じて登録データを受信する過程と、ネットワークを通じて登録データを配信装置に伝送する過程と、登録データに回答して処理装置でネットワークを通じて配信装置から暗号化された復号化鍵及び暗号化された仮想IDを受信する過程と、仮想IDを使用して暗号化された復号化鍵を復号化する過程と、及び復号化鍵を使用して暗号化されたプログラムを復号化する過程と、仮想IDを使用してプログラムを再復号化する過程と、暗号化された仮想ID及び復号化プログラムを第1記録デバイスに記録する過程とを含む所定の機能の実行が可能である。



【特許請求の範囲】**【請求項1】**

暗号化されたプログラムを受信するための装置であって、

ネットワークを通じて通信を行うためのネットワークインターフェースであって、(i) ネットワークを通じて機器IDが管理装置に送信され、(ii) 前記機器IDに応答して、ネットワークを通じて前記管理装置から登録データを受信し、(iii) ネットワークを通じて配信装置に前記登録データが送信され、かつ、(iv) 前記登録データに応答して、前記ネットワークを通じて暗号化された復号化鍵及び暗号化された仮想IDが配信装置から受信されるように前記通信を行うためのネットワークインターフェースと、

前記暗号化された復号化鍵の復号化、暗号化されたプログラムの前記復号化鍵を用いた復号化、及び前記仮想IDを用いての前記プログラムの再暗号化を行うための暗号化／復号化デバイスと、

前記暗号化された仮想IDと前記再暗号化されたプログラムとを記録するための第1記録デバイスと、を有する装置。

【請求項2】

前記ネットワークインターフェースは、前記機器IDと配信IDとを前記管理装置に前記ネットワークを通じて伝送可能で、かつ、前記機器ID及び前記配信IDに応答して、ネットワークを通じて前記管理装置から前記登録データを受信するよう動作可能なものである、請求項1記載の装置。

【請求項3】

前記登録データには、少なくとも前記機器IDと前記配信IDとのいずれかが含まれる、請求項2記載の装置。

【請求項4】

前記機器IDが前記装置に対して実質的に固有のものであり、前記仮想IDが前記機器IDと関連付けられている、請求項1記載の装置。

【請求項5】

前記暗号化／復号化デバイスは、前記暗号化された仮想IDの前記機器IDを用いた復号化、前記暗号化された復号化鍵の前記仮想IDを用いた復号化、前記暗号化されたプログラムの前記復号化鍵を用いた復号化、及び前記プログラムの前記仮想IDを用いた再暗号化を行うためのものである、請求項1記載の装置。

【請求項6】

前記第1記録デバイスは、更に前記機器IDを記録するためのものである、請求項5記載の装置。

【請求項7】

前記暗号化／復号化デバイスは、前記暗号化された仮想IDの前記機器IDを用いた復号化、及び前記装置が前記プログラムを実行することが可能となるように前記再暗号化されたプログラムの前記仮想IDを用いた復号化を行うためのものである、請求項6記載の装置。

【請求項8】

前記第1記録デバイスは、前記装置に対して着脱自在である、請求項6記載の装置。

【請求項9】

機器IDが記録された第2記録デバイスと、

前記第1記録デバイスに記録された機器IDを前記第2記録デバイスに記録された機器IDと比較し、かつ、両者が一致しない場合は、前記第1記録デバイスに記録された機器ID及び前記第2記録デバイスに記録された機器IDのいずれをも前記暗号化された仮想IDの復号化に使用することを禁止するためのプロセッサと、を更に有する、請求項6記載の装置。

【請求項10】

前記プロセッサは、更に、前記第1記録デバイスに記録された機器IDが前記第2記録デバイスに記録された機器IDと一致しない場合に、前記装置のユーザに対して、再関連

10

20

30

40

50

付けルーチンを選択する入力を促すように動作可能である、請求項9記載の装置。

【請求項11】

前記ネットワークインターフェースは、更に、

前記第2記録デバイスに記録された機器IDが前記第1記録デバイスに記録された機器IDと一致しない場合に、前記第2記録デバイスに記録された機器IDを前記ネットワークを通じて前記配信装置に伝送するよう動作可能で、かつ、

前記配信装置から前記ネットワークを通じて新たな暗号化された仮想IDを受信することが可能であり、前記新たな暗号化された仮想IDにおける前記仮想IDは、前記第2記録デバイスに記録された機器IDに関連付けられたものである、請求項9記載の装置。

【請求項12】

前記第1記録デバイスは、更に、前記新たな暗号化された仮想IDにより前記暗号化された仮想IDを置換するよう動作可能なものである、請求項11記載の装置。

【請求項13】

前記暗号化／復号化デバイスは、前記第2記録デバイスに記録された前記機器IDを用いての前記新たな暗号化された仮想IDの復号化、及び前記装置が前記プログラムを実行することが可能となるように前記仮想IDを用いての前記再暗号化されたプログラムの復号化を行うためのものである、請求項12記載の装置。

【請求項14】

前記ネットワークインターフェースは、更に、前記配信装置から前記ネットワークを通じて、前記暗号化されたプログラムを受信するためのものである、請求項1記載の装置。

【請求項15】

前記プログラムは、アプリケーションプログラムとシステムプログラムとのいずれかである、請求項1記載の装置。

【請求項16】

暗号化されたプログラムを処理装置で受信し、

機器IDをネットワークを通じて管理装置に伝送し、

前記管理装置から、前記機器IDにตอบสนองして、ネットワークを通じて前記登録データを受信し、

前記登録データを前記ネットワークを通じて配信装置に伝送し、

前記配信装置から、前記登録データにตอบสนองして、暗号化された復号化鍵と暗号化された仮想IDを前記ネットワークを通じて前記処理装置で受信し、

前記暗号化された復号化鍵を前記仮想IDを用いて復号化し、前記暗号化されたプログラムを前記復号化鍵を用いて復号化し、

前記プログラムを前記仮想IDを用いて再暗号化し、

前記暗号化された仮想IDと前記再暗号化されたプログラムとを第1記録デバイスに記録する、方法。

【請求項17】

前記機器IDと配信IDとを、ネットワークを通じて前記管理装置に伝送し、

前記ネットワークを通じて、前記機器IDにตอบสนองして、前記登録データを前記管理装置から受信する、請求項16記載の方法。

【請求項18】

前記登録データは、前記機器ID及び配信IDを含む、請求項17記載の方法。

【請求項19】

前記仮想IDが前記機器IDに関連付けられる、請求項17記載の方法。

【請求項20】

前記暗号化された仮想IDを前記機器IDを用いて復号化し、前記暗号化された復号化鍵を前記仮想IDを用いて復号化し、前記暗号化されたプログラムを前記復号化鍵を用いて復号化し、前記プログラムを前記仮想IDを用いて再暗号化する、請求項19記載の方法。

【請求項21】

10

20

30

40

50

前記機器 I D と前記暗号化された仮想 I D とを前記第 1 記録デバイスに記録する、請求項 20 記載の方法。

【請求項 22】

前記暗号化された仮想 I D を前記機器 I D を用いて復号化し、前記処理装置が前記プログラムを実行可能となるように、前記再暗号化されたプログラムを前記仮想 I D を用いて復号化する、請求項 21 記載の方法。

【請求項 23】

前記第 1 記録デバイスは、前記処理装置に対して着脱自在である、請求項 21 記載の方法。

【請求項 24】

前記処理装置は、前記機器 I D が記録された第 2 記録デバイスを有するものであり、
前記第 1 記録デバイスに記録された機器 I D を前記第 2 記録デバイスに記録された機器 I D と比較し、
これらの機器 I D 同士が一致しない場合は、前記第 1 記録デバイスに記録された機器 I D と前記第 2 記録デバイスに記録された機器 I D のいずれをも、前記暗号化された仮想 I D の復号化に使用することを禁止する、請求項 21 記載の方法。

【請求項 25】

前記第 1 記録デバイスに記録された機器 I D が前記第 2 記録デバイスに記録された機器 I D と一致しない場合に、前記装置のユーザに対して、再関連付けルーチンを選択する入力を促す、請求項 24 記載の方法。

【請求項 26】

前記第 2 記録デバイスに記録された機器 I D が前記第 1 記録デバイスに記録された機器 I D と一致しないときは、前記第 2 記録デバイスに記録された機器 I D を前記ネットワークを通じて前記管理装置に伝送し、
前記管理装置から新たな暗号化された仮想 I D を受信し、前記新たな暗号化された仮想 I D の前記仮想 I D は、前記第 2 記録デバイスに記録された前記機器 I D と関連付けられている、請求項 24 記載の方法。

【請求項 27】

前記暗号化された仮想 I D を前記第 1 記録デバイスに記録された新たな仮想 I D で置換する、請求項 26 記載の方法。

【請求項 28】

前記新たな暗号化された仮想 I D を前記第 2 記録デバイスに記録された機器 I D を用いて復号化し、
前記再暗号化されたプログラムを、前記処理装置が前記プログラムを実行可能となるように、前記機器 I D を用いて復号化する、請求項 27 記載の方法。

【請求項 29】

前記暗号化されたプログラムを前記配信装置から前記ネットワークを通じて受信する、請求項 16 記載の方法。

【請求項 30】

前記プログラムは、アプリケーションプログラムとシステムプログラムとのいずれかである、請求項 16 記載の方法。

【請求項 31】

ネットワークを通じて通信可能なネットワークインターフェースであって、(i) 前記ネットワークを通じて処理装置からそれぞれの機器 I D が受信され、(ii) 前記機器 I D に応答して、前記ネットワークを通じて管理装置から登録データが前記それぞれの処理装置に送信されるように前記通信を行うネットワークインターフェースと、
前記受信した機器 I D を記録するためのデータベースと、を備えた装置であって、
前記登録データは、暗号化された復号化鍵と暗号化された仮想 I D とをネットワークを通じて配信装置から入手するために前記処理装置により用いられるものであり、かつ、前記暗号化された復号化鍵は、前記仮想 I D を用いて前記処理装置により復号化でき、前記

10

20

30

40

50

暗号化されたプログラムは、前記復号化鍵を用いて前記処理装置により復号化できるものである装置。

【請求項32】

前記ネットワークインターフェースは、更に、暗号化されたプログラムとアクティベートされていない復号化鍵とを配信装置に伝送するためのものであり、前記アクティベートされていない復号化鍵は、アクティベートされた場合は、前記暗号化されたプログラムの復号化に使用できる、請求項31記載の装置。

【請求項33】

前記ネットワークインターフェースは、更に (i) 前記ネットワークを通じて前記配信装置からアクティベート要求を受信し、かつ、(ii) 前記アクティベート要求に応答して前記ネットワークを通じてアクティベート承認情報を前記配信装置に送信するためのものであり、前記アクティベート承認情報に応答して前記アクティベートされていない復号化鍵が有効化復号化鍵に変換可能である、請求項32記載の装置。

【請求項34】

前記ネットワークインターフェースは、更に (i) 実質的に固有の識別子である配信IDを含む復号化鍵管理データを前記配信装置に送信し、(ii) 前記配信装置から前記復号化鍵管理データ及び有効化要求を受信し、かつ、(iii) 前記復号化鍵管理データが有効であれば、アクティベート承認情報を送信するためのものである、請求項31記載の装置。

【請求項35】

ネットワークを通じて処理装置からそれぞれの機器IDを受信し、
前記機器IDに응答して前記ネットワークを通じて登録データを前記の処理装置に送信し、
前記受信した機器IDをデータベースに記録し、
前記登録データは、暗号化された復号化鍵と暗号化された仮想IDとを前記ネットワークを通じて配信装置から入手するために前記処理装置で使うことができるものであり、かつ、前記暗号化された復号化鍵は、前記処理装置で前記仮想IDを用いて復号化可能であり、更に、前記暗号化されたプログラムは、前記処理装置で、前記復号化鍵を用いて復号化可能である、方法。

【請求項36】

前記ネットワークを通じて、復号化されたプログラムとアクティベートされていない復号化鍵とを配信装置に送信し、前記アクティベートされていない復号化鍵は、アクティベートされた場合は、前記暗号化されたプログラムの復号化に用いることができるものである、請求項35記載の方法。

【請求項37】

更に (i) 前記ネットワークを通じて前記配信装置からアクティベート要求を受信し、
(i) 前記アクティベート要求に응答して前記ネットワークを通じて前記配信装置にアクティベート承認情報を伝送し、前記アクティベートされていない復号化鍵は、前記アクティベート承認情報に응答してアクティベートされた復号化鍵に変換可能である過程を含む、請求項36記載の方法。

【請求項38】

更に (i) 実質的に固有の識別子である配信IDを含む復号化鍵管理データを前記配信装置に伝送し、(ii) 前記復号化鍵管理データとアクティベート要求とを前記配信装置から受信し、(iii) 前記復号化鍵管理データが有効であれば、前記アクティベート承認情報を送信する、請求項35記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、プログラムコンテンツのセキュアな配布方法及び装置に関し、これらの方法及び装置は、上記プログラムコンテンツの不正なコピーや配布を防ぐためのものである。

【背景技術】**【0002】**

プログラムコンテンツとしては、ビデオゲームのゲームプログラム、ワードプロセッサのプログラム、表計算のプログラムや、オペレーティングシステム等のシステムプログラムやブートプログラム等が挙げられる。

コンピュータプログラム等のプログラムコンテンツは、通常、これらのプログラムコンテンツが記録されたCD-ROMやDVD-ROM等の輸送可能な記録媒体というかたちでエンドユーザに対して配布される。また、インターネットを通じてサーバからユーザがダウンロードする形態でプログラムコンテンツを配布する場合もある。

【発明の開示】**【発明が解決しようとする課題】****【0003】**

従来のプログラムコンテンツの配布方法は、不正コピーがなされて複数のエンドユーザに行き渡ってしまうということから、セキュアなもの、つまりセキュリティ性を備えたものとはいえなかった。例えば、コンピュータプログラムプログラムが特定のエンドユーザに対して記録媒体に記録された形態で配布された場合、そのユーザが、他のエンドユーザが使用する機器に、配布されたコンピュータプログラムを不正コピーする場合は挙げられる。通常これらの不正コピーは、ハードディスク、CD-ROM等に記録される。同様に、コンピュータプログラムがネットワークを通じてエンドユーザに配布された場合もコンピュータプログラムが不正コピーされて他のユーザに配布されるおそれがある。例えば、コンピュータプログラムが正規のエンドユーザの使用する機器に記録された後に、そのユーザがコンピュータプログラム記録媒体（例えば、光ディスク、磁気ディスク等）に記録した形態でコピーし、あるいは電子メールに添付して他のユーザにわたす場合もある。

【0004】

従って、プログラムコンテンツのセキュアな配布を行うための新規な方法及び装置であって、プログラムコンテンツの不正コピーの増殖に関する問題を改善できるものが必要とされている。

【課題を解決するための手段】**【0005】**

本発明の一つ以上の態様によれば、暗号化されたプログラムを受信するための装置であって、ネットワークを通じて通信を行うためのネットワークインターフェースであって、（i）ネットワークを通じて機器IDが管理装置に送信され、（ii）前記機器IDに回答して、ネットワークを通じて管理装置から登録データを受信し、（iii）ネットワークを通じて配信装置に前記登録データが送信され、かつ、（iv）前記登録データに回答して、前記ネットワークを通じて暗号化された復号化鍵及び暗号化された仮想IDが配信装置から受信されるように前記通信を行うためのネットワークインターフェースと、前記暗号化された復号化鍵の復号化、暗号化されたプログラムの前記復号化鍵を用いた復号化、及び前記仮想IDを用いた前記プログラムの再暗号化を行うための暗号化／復号化デバイスと、前記暗号化された仮想IDと前記再暗号化されたプログラムとを記録するための第1記録デバイスと、を有する装置が提供される。

【0006】

好適には、前記ネットワークインターフェースは、前記機器IDと配信IDとが前記管理装置に前記ネットワークを通じて伝送され、かつ、前記前記機器ID及び配信IDに回答して、ネットワークを通じて前記管理装置から前記登録データを受信するためのものである。

【0007】

好適には、前記識別情報は、実質的に機器毎に固有の機器IDを含み、前記仮想IDは、前記機器IDと関連づけられている。好適には、前記暗号化／復号化デバイスは、前記暗号化された仮想IDの前記機器IDを用いた復号化、及び前記装置が前記プログラムを実行することが可能となるように前記再暗号化されたプログラムの前記仮想IDを用いた

10

20

30

40

50

復号化を行うためのものである。前記第1記録デバイスは、更に前記機器IDを記録することが可能である。

【0008】

前記復号化装置は、前記暗号化された仮想IDを前記機器IDを用いて復号化することが可能であり、かつ、前記仮想IDを用いて再復号化されたプログラムを実行可能とすることが望ましい。

【0009】

前記装置は、更に機器IDが記録された第2記録デバイスと、第1記録デバイスに記録された機器IDと前記第2記録デバイスに記録された前記機器IDとを比較し、これら機器ID同士が一致しない場合は、いずれの前記記録デバイスに記録された機器IDも暗号化された仮想IDの復号化のために使用を禁止することが可能であるプロセッサと、を含む。

10

【0010】

前記プロセッサは、好適には、前記第1記録デバイスに記録された機器IDが前記第2記録デバイスに記録された機器IDと一致しない場合に、前記装置のユーザに対して、再関連付けルーチンを選択する入力を促す、あるいは入力画面を表示して上記関連付けルーチンを選択するための入力を可能とする。前記ネットワークインタフェースは、好適に前記第2記録デバイスに記録された機器IDが前記第1記録デバイスに記録された機器IDと一致しない場合に、配信元である前記配信装置にネットワークを通じて前記機器IDを伝送し、前記第2記録デバイスに記録された機器IDと関連している新たに暗号化復号化された仮想IDをネットワークを通じて前記配信装置から受信するためのものである。好適には、前記第1記録デバイスは、前記暗号化された仮想IDを前記新たに暗号化された前記仮想IDにより置換が可能である。前記復号化装置は、第2記録デバイスに記録された前記機器IDを用いて新たに暗号化された前記仮想IDを復号化し、かつ、前記装置が前記再暗号化されたプログラムの実行が可能であるような前記仮想IDを用いて再暗号化されたプログラムの復号化が可能であることが好ましい。

20

【0011】

本発明の更なる1つ以上の様態によれば、暗号化されたプログラムを処理装置で受信する過程と、機器IDをネットワークを通じて管理装置に伝送する過程と、前記管理装置から、前記機器IDに応答して、ネットワークを通じて前記登録データを受信する過程と、前記登録データを前記ネットワークを通じて配信装置に伝送する過程と、前記配信装置から、前記登録データに応答して、暗号化された復号化鍵と暗号化された仮想IDを前記ネットワークを通じて前記処理装置で受信する過程と、前記暗号化された復号化鍵を前記仮想IDを用いて復号化し、前記暗号化されたプログラムを前記復号化鍵を用いて復号化する過程と、前記プログラムを前記仮想IDを用いて再暗号化する過程と、前記暗号化された仮想IDと前記再暗号化されたプログラムを第1記録デバイスに記録する過程と、を含む方法が提供される。

30

【0012】

前記方法は、更にネットワークを通じて機器IDと配信IDを管理装置に伝送し、及びネットワークを通じて管理装置から前記機器IDと配信IDに応答しての登録データを受信する過程と、を含む。

40

【0013】

好適には、前記方法は、前記暗号化された仮想IDを前記機器IDを用いて復号化する過程と、前記暗号化された復号化鍵を前記仮想IDを用いて復号化する過程と、前記暗号化されたプログラムを前記復号化鍵を用いて復号化する過程と、前記プログラムを前記仮想IDを用いて再暗号化する過程と、を含む。前記方法は更に前記機器IDを使用して、前記暗号化された仮想IDを復号化する過程と、及び前記処理装置が前記プログラムの実行可能となるように、前記仮想IDを使用して、前記再復号化されたプログラムを復号化する過程と、を含む。

【0014】

50

前記方法は、好適には、第1記録デバイスに記録された機器IDと第2記録デバイスに含まれる前記機器IDとを比較する過程と、これら機器IDが一致しない場合、前記暗号化された仮想IDを復号化するためのどちらの記録デバイスにも含まれる機器IDの使用を禁止する過程と、を更に含む。

【0015】

本発明の1つ以上の形態に係る装置では、管理装置から暗号化されたプログラム及びアクティベートされていない復号化鍵とを受信可能である入力インタフェースを有し、前記アクティベートされていない復号化鍵は、アクティベートされた場合、暗号化されたプログラムを復号化するために使用可能であり、入力インターフェースを有し、この入力インターフェースは、(i) ネットワークを通じて管理装置にアクティベート要求を伝送し、

(ii) ネットワークを通じて管理装置から前記有効化要求に応答してのアクティベート承認情報を受信可能であるような通信を行うためのものであり、データプロセッサを有し、このデータプロセッサは、前記アクティベート承認情報に応答して前記アクティベートされていない復号化鍵をアクティベートされた復号化鍵に変換するものであり、更に、データベースを有し、このデータベースは、複数の復号化プログラムに対応するそれぞれの復号化鍵を記録するものである。

【0016】

好適には、前記入力インタフェースは、更に(i) 実質的に固有の識別子である配信IDを含む復号化鍵管理データを管理装置から受信し、(i) 前記復号化鍵管理データ及びアクティベート要求を管理装置に伝送し、及び(iii) 前記復号化鍵管理データが有効であれば、前記アクティベート承認情報を受信するよう動作可能である。前記アクティベートされていない復号化鍵は、元々暗号化された復号化鍵であり、前記データプロセッサは、前記アクティベート承認情報を使用して、前記暗号化された復号化鍵を復号するよう動作可能である。

【0017】

前記ネットワークインタフェースは、それぞれの処理装置に関連する登録データがネットワークを通じて処理装置から受信されるよう動作可能である。前記データベースは、それぞれ処理装置の一つに関連する各機器IDの記録が可能である。前記データプロセッサは、更に、前記データベースから、受信した登録データのいずれかに一致する機器IDを索出するよう動作可能であり、前記ネットワークインタフェースは、更に、前記受信した登録データに回答して、ネットワークを通じて、暗号化されたアクティベートされた復号化鍵を前記処理装置に伝送するよう動作可能であり、前記アクティベートされた復号化鍵は処理装置に施されている暗号化プログラムを復号化するために使用可能である。

【0018】

前記登録データは、対応する処理装置に対して実質的に固有の機器IDを含み、前記データプロセッサは、前記機器IDに回答して、暗号化されたアクティベートされた復号化鍵を生成するよう動作可能である。好適には、前記データプロセッサは、仮想IDを、前記機器IDの関数として前記機器IDと関連付けられるように生成し、前記アクティベートされた復号化鍵を前記仮想IDを用いて暗号化し、かつ、前記仮想IDを前記機器IDを用いて暗号化するよう動作可能である。前記ネットワークインタフェースは、前記暗号化された仮想IDを、前記ネットワークを通じて前記処理装置に対して伝送するよう動作可能である。

【0019】

本発明のさらなる1つ以上の形態に係る装置は、(i) ネットワークを通じて処理装置からそれぞれの機器IDを受信し、(ii) 前記機器IDに回答して登録データがネットワークを通じてそれぞれの処理装置に伝送されるようにネットワークとの通信を行うネットワークインタフェースと、前記受信した機器IDを記録するデータベースと、を有する。前記登録データは、前記処理装置によって、暗号化された復号化鍵及び暗号化された仮想IDをネットワークを通じて配信装置から得るために使用されるものであり、前記暗号化された復号化鍵は、前記仮想IDを用いて前記処理装置によって復号化可能なものであり

、前記暗号化されたプログラムは、前記復号化鍵を持って前記処理装置によって復号化可能なものである。

本発明の1つ以上のさらなる形態によると、上記装置により実行される1つ以上の動作を実現するための1つ以上の方法が考えられる。

本発明のさらなる様態、機能、効果等は、以下の説明及び添付図面等を参照すれば、この技術分野の当業者には明らかになる。

また、本発明を図示するために、現段階で好適な形態で図面を示すが、本発明は図示される手段や配置に限定されるものではないことを理解されたい。

【発明を実施するための最良の形態】

【0020】

図1に、プログラムコンテンツを複数のエンドユーザに対して、セキュアに配布すること、例えば、プログラムコンテンツの不正なコピーが防止されるか、あるいは使用不能な状態とされるように配布することが可能なシステム10を示す。なお、図中において、同じ要素には同じ番号を付して説明した。このシステム10においては、好ましくは、サードパーティサーバ1と、暗号化サーバ2と、配信サーバ3と、管理サーバ4及び複数のクライアント端末5と、を含み、これらは、例えばインターネット6を通じて接続されている。なお、システム10において、本発明の範囲を逸脱することなく、サードパーティサーバ1、暗号化サーバ2、配信サーバ4及び／又は管理サーバ4を複数設けることもできる。以下、簡素化のために、各サーバをそれぞれ一台のみ示して説明する。

各サーバ1、2、3、4は、好適には、個人やエンティティ(entity:装置、会社、財団、法人、あるいはその他の組織等であり、以下、単に「組織」と記載する)による維持や操作、及び／又は個人や組織に対してその他の関連づけがなされている。なお、サーバおよびそのサーバに関連付けられた組織に対する参照符号は、相互に入れ替えてもよい。

【0021】

サードパーティサーバ1は、好適には、操作、維持、及び／又はその他の関連づけが、例えばプログラムコンテンツのディベロッパーと関連づけられた組織に対してなされている。一例として、サードパーティサーバ1は、コンピュータアプリケーションプログラム、コンピュータシステムプログラム等のディベロッパーとしてもよい。好適にはサードパーティサーバ1は、本発明の範囲から逸脱することなく、他の組織と関連付けられる、サードパーティサーバ1は、サーバに関連する機能を実行するための公知の(又はこれから開発される)ハードウェアを用いて構築することが可能である。

【0022】

暗号化サーバ2は、好適には、維持、操作、及び／又は管理機能を実行できる組織に関連付けられている(その詳細は後述する)。好適にはこの組織は、前記管理サーバ4と同じ組織である。しかしながら、前記暗号化サーバ2は、本発明の範囲を逸脱することなく、他の組織と関連付けられる。前記暗号化サーバ2はサーバに関連する機能を実行するための公知(又はこれから開発される)のハードウェアのいずれを用いて構築してもよい。

【0023】

配信サーバ3は、好適には、ネットワーク6の方法のようにクライアント端末5に前記プログラムを送送することを実行できる組織によりコントロール、維持、及び／又は関連づけがなされる。しかしながら、前記プログラムは、記録メディアのような他のメディアを通じて伝送するようにしてもよい。前記配信サーバ3は好適に後に詳細が記載されるパーソナライジングデータベース7に接続される。前記配信サーバ3及びパーソナライジングデータベース7は、ネットワークサーバ関連機能を実行するために適用されるいずれの公知の(又はこれから開発される)ハードウェアをも使用して構築してもよい。

【0024】

管理サーバ4は、好適には、所定の管理機能を実行することができる組織により維持、コントロール、及び／又は関連づけがなされる(その詳細は後述する)。管理サーバ4はネットワークサーバ機能及びデータベース機能を実行するために適用される、公知の(又はこれ以後開発された)ハードウェアのいずれを使用して構築してもよい。

【0025】

以下の記載から明らかであるように、サードパーティサーバ1、暗号化サーバ2、配信装置としての配信装置サーバ3及び管理サーバ4により実行されるそれぞれの機能は、それらサーバを操作または維持し、及び／またはその他関連付けがなされた1つ以上のサーバ間及び／又は1つ以上の組織に割り当てることができる。実際、それぞれのサーバに対して個別に組織を割り当てることが要求されるわけではなく、例えば、1つの組織が暗号化サーバ3と管理サーバ4に関連付けられてもよい。しかし、上述の機能の分配は、好適には図1に示すものと一致するようになされる。

【0026】

概略的には、それぞれのクライアント端末5は、好適にはハードディスクドライブ8、及びソニーメモリスティックのようなメモリカード9等の、公知のいずれのハードディスクドライブウェアにも動作可能であるように接続される。ハードディスクドライブ8とメモリカード9（好適にはクライアント端末5に着脱自在であるように接続される）は、装置5では別個のアイテムとして示されているが、それらは本発明の趣旨及び範囲から逸脱することなしに両者を一体のものとして装置5に配置してもよい。クライアント端末5は、パーソナルコンピュータ、ソニープレイステーション2等の公知のハードウェアのいずれを使用して構築してもよい。

【0027】

本発明の1つ以上の形態によれば、クライアント端末5は、好適にはCD-ROM、DVD-ROM、電子メモリのような記録メディアを通じて、又はネットワーク6を通じてプログラムをダウンロードすることにより、コンピュータアプリケーションプログラムのような暗号ソースコンピュータプログラムの受信が可能である。暗号ソースコンピュータプログラムは、本発明の趣旨及び範囲から逸脱することなく、正規の会社のいずれから入手することができるが、好適には、クライアント端末5は、暗号ソースプログラムを配信サーバ3から（ネットワーク6を通じてダウンロードすることにより）、又は、ソフトウェアディベロッパ及び／又は配信サーバ3と直接的及び／又は間接的に関連する従来の実店舗型の配信元から受信する。クライアント端末5は、またソース暗号ソースコンピュータプログラムを特定の組織から受信することは要求されず、実際、管理サーバ4、サードサーバ1又は他の組織から受信してもよい。

【0028】

本実施形態の利点としては、エンドユーザは、クライアント端末5で最初に復号化鍵を入手して暗号ソースコンピュータプログラムを復号化しなければプログラムを実行できない形式（ソース暗号化）で、コンピュータプログラムを受信するということが挙げられる。更に、暗号化されたコンピュータプログラムが、認可されたコピーを通じて入手された場合、不正利用をしようとするエンドユーザは、最初に復号化鍵を入手しなければプログラムを実行できないであろう。下記に詳細を記載するように復号化鍵は認可されたクライアント端末5のみにより入手可能である。

【0029】

図2に、暗号化サーバ2及びサードパーティサーバ1により実行される所定の処理ステップを示す概念的ブロック図とフロー図を示す。この図により、暗号ソースコンピュータプログラムがどのように生成されるかの一例が示される。この例において、サードパーティサーバ1は、ソフトウェアディベロッパに関連付けられており、このソフトウェアディベロッパ自体又は関連する他の組織が、コンピュータシステムプログラム、コンピュータアプリケーションプログラム等のようなプログラムを入手する。図2に示すようにサードパーティサーバ1は少なくとも1つのシステムプログラム及び少なくとも1つのアプリケーションプログラムを有する。これら1つ以上のプログラムは暗号化サーバ2にネットワークを通じて伝送される。しかし、プログラムは、例えば記録メディアを通じて暗号化サーバ2に手動で提供される。

【0030】

暗号化サーバ2は好適にプログラムを復号化し、暗号化されたプログラムをサードパー

10

20

30

40

50

ティサーバ1に返信する。暗号処理は、暗号化されたプログラムを生成するために公開鍵暗号化、共通鍵暗号化等のようないずれの公知の暗号技術を採用してもよい。この例では、暗号化サーバ2は、暗号化されたシステムプログラム（ソース暗号化プログラム）及び暗号化されたアプリケーションプログラム（暗号ソースアプリケーションプログラム）をサードパーティサーバ1に返信する。本発明の実施に必須ではないが、暗号化サーバ2は暗号化されたプログラムを復号化することが可能な復号化鍵をサードパーティサーバ1に提供するようにしてもよい。好適には、復号化鍵は、アクティベートされていない状態で、つまり暗号ソースプログラムを容易に復号化できないようにして配信サーバ3に提供される。例えば、復号化鍵は、最初に、例えば暗号化サーバ2により、アクティベートされていない状態となるように暗号化される。このことにより、以下に記載するようにセキュリティのレベルを向上される。

10

【0031】

以下記載するようにサードパーティサーバ1は、暗号化されたプログラムを配信サーバ3に対して記録メディアを通じて手動により配布するか、あるいはネットワーク6を通じて電子的にダウンロードすることで配布する。暗号ソースプログラムがどのように配布されるかに係わらず、エンドユーザは、好適には、以下に記載するように所定の登録手段を実施しなければプログラムを実行できないようになっている。

【0032】

配信サーバ3と管理サーバ4で好適に実行される処理ステップを表す概念的ブロック図及びフロー図を図3に示す。配信サーバ3は好適にネットワーク6を通じて管理サーバ4と通信リンクを構築する。管理サーバ4は、好適にネットワーク6を通じて鍵配信プログラム11、鍵管理データ12及び鍵登録プログラム13を配信サーバ3に伝送する。後述するように、鍵配信プログラム11は、エンドユーザに対する復号化鍵の配信を許可するために配信サーバ3を通じて実行される。鍵管理データは、好適に情報のセキュアな集合であり、実質的に個々の配信サーバ3に固有である配信IDを含む。以下でより詳細に記載するが、鍵登録プログラム13は、非アクティブな復号化鍵をアクティブな復号化鍵（つまり暗号ソースコンピュータプログラムの復号化に使用可能である）に変換するために配信サーバ3により好適に実行される。

20

【0033】

図4に、配信サーバ3と管理サーバ4との間で好適に実行される更なる処理ステップを示すフローチャートを示す。概略的には、配信サーバ3はネットワーク6を通じて管理サーバ4にアクティベート要求を実行し、これに応答して管理サーバ4からアクティベート承認情報を受信する。より詳細には、ステップS1において配信サーバ3は、好適にネットワーク6を通じて管理サーバ4と通信の接続をする。ステップS2において、配信サーバ3は、管理サーバ4に鍵管理データ（配信IDを含む）を伝送する。

30

【0034】

ステップS3において管理サーバ4は、適切な認証処理プロセスを使用して配信サーバ3を好適に認証する。例えば、管理サーバ4は、配信サーバ3が認証許可を提供するためのユーザID、パスワード等、又は他の認証可能な情報の提供の要求をするようにしてもよい。しかしながら、好適には、管理サーバ4は配信サーバ3を認証するために、鍵管理データ12から配信IDを抽出する。ステップS4において、認証が成功したかどうか判定される。認証が成功しなかった場合、ステップS5への処理に進み、アクティベートは許可されず、処理も終了する。認証が成功した場合、好適にS6の処理へと進み、ここではアクティベート承認情報が管理サーバ4からネットワーク6を通じて配信サーバ3に伝送される。

40

【0035】

ステップS7において、配信サーバ3は好適に暗号ソースコンピュータプログラムに関連した復号化鍵をアクティベートする。より詳細には、配信サーバ3はアクティベート承認情報を入力として要求する鍵登録プログラム13を好適に実行する。これに応答して鍵登録プログラム13は、暗号ソースコンピュータプログラムの復号化に使用できるように

50

復号化鍵を有効化する。一例として、アクティベート承認情報には、予め暗号化された復号化鍵の復号化に適用できる復号化鍵を有する。この場合、鍵登録プログラム13は、予め暗号化された復号化鍵をアクティベート承認情報を用いて復号化が可能なものとなっている。

【0036】

復号化鍵がどのようにアクティベートされたか、また、アクティベートがなされたか否かにかかわらず、配信サーバ3は、好適にパーソナライジングデータベース7内に復号化鍵を記録する。この段階において、配信サーバ3は、暗号ソースコンピュータプログラムとそのようなプログラムの復号化が可能な復号化鍵とを有すること（もしくはこれらにアクセスできる状態）となる。

【0037】

暗号ソースコンピュータプログラムの処理のために好適に実行される所定のステップを示す概念的ブロック及びフローの説明図を図5に示す。図5に示すように、クライアント端末5は、好適にネットワーク6を通じてのダウンロード又はCD-ROM10のような記録媒体を通じて暗号ソースコンピュータプログラムを受信済みである。クライアント端末5は、配信サーバ3から暗号ソースコンピュータプログラムを入手済みであることが好ましい。しかしながら、暗号ソースコンピュータプログラムを実行するためには、クライアント端末5は所定の登録ステップを実行しなくてはならない。これらのステップは、好適にネットワーク6を通じて管理サーバ4を示して説明される。

【0038】

図6のフローチャートに、登録プロセスの一部を示す。ステップS20において、クライアント端末5は上記したように暗号ソースコンピュータプログラムを受信して後述するように記録する。ステップS22において、ユーザは、コンピュータプログラムをインストールして使用可能状態とする意思を示す命令を好適に入力する。これに関してクライアント端末5は、好適には、ユーザのインストール指示に応答して起動するプログラムを有する。このプログラムは、ユーザに暗号化コンピュータプログラムの登録の入力を受け付ける状態となること等によって登録を促し、通信機能を起動させる（ステップS24）。

【0039】

クライアント端末5は、好適には、ネットワーク6を通じて技術分野において公知の通信可能なネットワークインタフェースを有する。実際、この目的のために公知のいずれのネットワークインタフェースハードウェアを採用してもよい。ステップS26において好適にクライアント端末5により通信経路形成が開始され、端末5と管理サーバ4間に当該通信経路が確立される。クライアント端末5のネットワークインタフェースは、好適にネットワーク6を通じて端末5に関連付けられた少なくとも何らかの識別情報を管理サーバ4に送信することを容易に可能にする。詳細には、識別情報は、好適には実質的にクライアント端末5に固有である機器IDを含む。識別情報は、暗号ソースプログラムの入手元（配信サーバ3）を示す配信IDを含むものとしてもよい。

【0040】

好適には、クライアント端末5は、暗号ソースプログラム及び後述する所定の他の情報を記録可能であるハードディスクドライブ8、メモリカード9等の第1記録デバイスと、機器IDの記録が可能であるROMのような第2記録デバイスと、を含む。好適には、クライアント端末5のネットワークインターフェースは、更に、ネットワーク6を通じて機器IDを（ROMから）管理サーバ4に伝送可能なものとなっている（動作ステップS28）。

【0041】

動作ステップS30において、管理サーバ4は、好適には登録データを再生してネットワーク6を通じてクライアント端末5に伝送する。例として登録データは、機器ID及び配信IDにより構築され、好適には、これらのIDは、その後の登録データの適切な分析により識別される。登録データを受信すると、クライアント端末は、好適にハードディスクドライブ及び／又はメモリカード9のような第1記録デバイスに同データを記録する。

10

20

30

40

50

【0042】

図7において、管理サーバ4は、データベース7Aに接続できることが示される。データベース7Aは、上記登録処理段階で受信されたデバイスID及び／又は配信IDも含むようにしてもよい。好適には、デバイスID及び配信IDは、有用な履歴データ及び分析が入手されるように互いに関連付けられて記録される。例えば、上述の分析から、あるクライアント端末5が、ある配信サーバ3から暗号ソースコンピュータプログラムを受信済みの状態になったと判定することもできる。配信サーバ3から入手したデータに関連して（以下更に記載する）、デバイスID、配信ID及び／又はこれらID間の関連付けは、配信サーバ3側における義務条項（例えば契約による）がすべて満たされていることを保証するように用いることもできる。

10

【0043】

図8と図9は、それぞれコンピュータプログラムを登録してエンドユーザによる実行を可能とするために好適に実行される更なる処理ステップを示す概念ブロック図及びフローチャートである。ユーザは、好適には、暗号ソースコンピュータプログラムを復号化するために適切な復号化鍵を入手するという意志表示をクライアント端末5に対して行う。ステップS21において、クライアント端末5は、ネットワーク6を通じて配信サーバ3と通信リンクを確立する。その後、クライアント端末5は、配信サーバ3に（予め管理サーバ4から入手された）登録データを伝送する（動作ステップS22）。

【0044】

動作ステップS23において、配信サーバ3は、ネットワーク6を通じてクライアント端末5から例えば機器IDを含む（配信元IDを含んでもよい）登録データを受信する。これに関して、配信サーバ3は、好適にはネットワーク6を通じてクライアント端末5から登録データを受信できるように通信を行うためのネットワークインタフェースを含む。ステップS23において、管理サーバ4は、また、他のID、ここでは仮想IDと呼ぶIDを割り当て、この仮想IDは、好適には、クライアント端末5から受信した機器IDに対応する。仮想IDは、既存の複数のIDから選択してもよく、また、機器ID、配信ID及び又はその他の演算対象に対する数値演算で得るようにしてもよく、あるいは、その他公知のあるいはこれから開発される技術を用いて仮想IDを生成してもよい。

20

【0045】

配信サーバ3は、パーソナライジングデータベース7から、クライアント端末5から受信した機器ID（つまり第2記録デバイス（ROM）に記録された機器ID）に一致する既存の機器IDを索出する。図10を参照するとパーソナライジングデータベース7は、好適には、それぞれのクライアント端末5に対応するそれぞれの機器IDの記録が可能である。図10の左欄に示すようにパーソナライジングデータベース7には複数の機器IDが予め記録されている。これら個々の機器IDは、クライアント端末5のうちの1つと関連付けられ、そしてそのような機器IDは、実質的にそれぞれのクライアント端末5に対して固有であることが好ましい。好適には、配信サーバ3もネットワーク6を通じてクライアント端末5から受信した機器IDに一致する登録情報（例えば機器ID）に関するパーソナライジングデータベース7を検出できるデータプロセッサを好適に含む。公知の又はこれから開発されるデータプロセッサハードウェアのいずれをもこの目的のために採用してよい。

30

40

【0046】

再度図9を参照すると、ステップS23では、仮想IDは、パーソナライジングデータベース7に記録された機器IDに関連付けられている。つまり、受信した機器IDを配信サーバ3に伝送する特定のクライアント端末5に対して、仮想IDが関連付けられている。この関連付けは、記録された機器IDに対応するように仮想IDをパーソナライジングデータベース7内に記録することにより達成される。例えば、クライアント端末5から受信された機器IDがK2345（図10）であり、生成された仮想IDがB5678である場合、機器IDK2345と仮想IDB5678の関連付けは、パーソナライジングデータベース7内における記録された機器IDK2345に対応する（又はリンクされた）

50

位置に仮想IDB5678を記録することで達成される。同様に、受信された機器IDがK6789であり、かつ再生された仮想IDがB9012であれば、機器IDK6789と仮想IDB9012の関連付けは、パーソナライジングデータベース7内の機器IDK6789に関連付けられた位置に仮想IDB9012を記録することで達成される。

【0047】

機器IDK1234とK0987の反対の位置にある仮想ID内の“--”は、関連するクライアント端末5がエンドユーザによりまだ購入されていないか、又はそのようなエンドユーザが、配信サーバ3によるコンピュータプログラムの登録をまだ行っていないことを示す。

【0048】

上記したように、クライアント端末5からネットワーク6を通じて配信サーバ3に伝送された（ステップS22、図9）登録データは、暗号ソースプログラムが入手される配信サーバ3に対応する配信IDを含んでも良い。本発明の他の実施形態では、登録データ内に含まれる配信IDは、機器IDと関連付けられてパーソナライジングデータベース7にも記録される。

【0049】

図9に示されるように、配信サーバ3は、好適には、暗号化された復号化鍵及び暗号化された仮想IDを生成するよう動作可能であり、ここで、復号化鍵はクライアント端末5で暗号ソースコンピュータプログラムを復号化するために用いられるものである。配信サーバ3は、暗号化サーバ2（図1～図2）により生成されたそれぞれの暗号ソースコンピュータプログラムを復号化するために使用される復号化鍵がいくつであっても、これらの復号化鍵にアクセスできるようにしてもよい。これら復号化鍵は暗号化サーバ2及び／又は他の適切な組織を通じて配信サーバ3に提供される。更に、これらの復号化鍵は、ネットワーク6及び他のネットワークを通じて、又は記録メディア等を通じて手動で配信サーバ3に提供される。

【0050】

ステップS24において、配信サーバ3は、好適には、クライアント端末5と関連する仮想IDを使用して復号化鍵を暗号化する。更に、配信サーバ3は、仮想IDを、クライアント端末5の関連付けられた機器IDを使用して暗号化する。これらの仮想ID及び機器IDは、好適には、パーソナライジングデータベース7からそれぞれが入手される。

【0051】

配信サーバ3のネットワークインタフェースは、好適には、ネットワーク6を通じて、暗号化された復号化鍵、及び暗号化された仮想IDの伝送（ステップS25）をクライアント端末5に伝送するためのものとなっている。ステップS26では、クライアント端末5は、好適には、暗号化された復号化鍵及び暗号化された仮想IDをネットワークを通じて受信し、そして第1記録デバイス（ハードディスクドライブ8、メモリカード9等）に記録する。動作ステップS27では、配信サーバ3は、好適に特定の復号化鍵がクライアント端末5に伝送されたことを（履歴データとして）記録する。この情報は、好適には、後に例えばネットワーク6を通じて、管理サーバ4に提供される。好適には、配信サーバ3は、履歴データに含まれているデータにアクセスすることができない。このデータは、決済目的のためや、債務関係の追跡等に使用される。

【0052】

本実施形態の利点としては、暗号化された復号化鍵は、正規のクライアント端末5のみに提供されるということが挙げられる。正規のクライアント端末5として、例えば、有効な機器IDを有し、復号化鍵を暗号化するために使用する仮想IDと関連する機器IDを登録したクライアント端末5が挙げられる。更に、ネットワークの不正行為又は不正コピー等によって、暗号化された復号化鍵を傍受しても、暗号ソースコンピュータプログラムを復号化するために必要な情報（即ち、使用可能な復号化鍵）を得ることはできない。実際、そのような復号化鍵は、実質的に固有である仮想IDにより暗号化される。同様に、暗号化されたその仮想IDは、登録処理が完了してクライアント端末5が認可されたとき

10

20

30

40

50

なされた後にのみクライアント端末機器5に提供される。仮想IDが、配信サーバ3からクライアント端末5に暗号化された手法（即ち、クライアント端末5の機器IDを使用する手法）で配信サーバ3から伝送されるので、暗号化された仮想IDをどのように不正に入手しても、暗号化された復号化鍵を復号化するために必要な情報は得られない。

【0053】

暗号ソースコンピュータプログラムをクライアント端末5内にロード／インストールするために実行される所定の処理を図11と図12に示す。図11においては、クライアント端末5は第1記録デバイス、つまりハードディスク8、メモリカード9等とは別個のものとして示される。しかしながら、上記したようにこれらの構成要素は本発明の請求項の趣旨と範囲から逸脱することなく、一体又は半一体な状態とすることもできる。プロセスのこの段階において、クライアント端末5は、第2デバイス、例えばROM、に記録された機器IDを含み、一方、第1記録デバイス8、9には、機器ID、暗号化された仮想ID、暗号化された復号化鍵、及び暗号ソースコンピュータプログラムが記録されている。

【0054】

ステップS50（図12参照）において、ユーザは、将来の使用のために暗号ソースコンピュータプログラムをロード／インストールするための指示をクライアント端末5に提供する。これにตอบสนองしてクライアント端末5は、適切なハードウェア及びソフトウェアを使用して第1記録デバイス8、9から機器IDを読み取り、第2デバイス、すなわちROMから機器IDを読み取る（ステップS52）。ステップS54において、これらの機器IDが一致するか否かが判定される。これらが一致しない場合、処理は終了し、及び／又はその他の処理に入る。しかしながら、これらが一致した場合、ステップS56に進み、暗号化された仮想IDを、機器ID（好適にはROMに記録された機器ID）を使用して復号化する。仮想IDが入手された後に、暗号化された復号化鍵は仮想IDを使用して復号化される（ステップS58）。次に暗号ソースコンピュータプログラムが復号化鍵を使用して復号化される（ステップS60）。ステップS62では、ステップS56で入手された仮想IDを使用してコンピュータプログラムが再度暗号化され、クライアントで暗号化されたコンピュータプログラムが得られる。このクライアントで暗号化されたコンピュータプログラムは、第1記録デバイス8、9内に記録される（ステップ64）。この段階では、暗号化された復号化鍵も暗号ソースコンピュータプログラムも第1記録デバイス8、9に保存される必要はない。

【0055】

クライアント端末5は、好適には、上記したように暗号化／復号化機能を実行するために暗号化デバイス及び復号化デバイスを含む。暗号化デバイス及び復号化デバイスは、一体のものとしてもよく、簡単のため復号化デバイスと称する。このような暗号化／復号化を実行するために公知の又はこれから開発されるいずれのハードウェア及び／又はソフトウェアをも本発明に用いることができる。例えば、復号化ライブラリー、暗号化ライブラリー等を用いることができる。

【0056】

本実施形態では、クライアント暗号化コンピュータプログラムはセキュアなものであるという利点がある。何故ならば（以下に説明されるように）他のクライアント端末5において不正なエンドユーザが不正なコピーを実行することはできないからである。実際、クライアントで暗号化されたコンピュータプログラムは、最初に復号化されなくてはならないが、以下に説明するように、このような復号化は、配信サーバ3によりコンピュータプログラムを登録されたクライアント端末5以外では実行することはできない。

【0057】

クライアント端末5により実行されるコンピュータプログラムの処理を図13、14を参照して説明する。この処理段階では、クライアント端末5は、機器IDが記録された第2記録デバイス、例えばROMと、機器ID、暗号化された仮想ID、クライアントで暗号化されたコンピュータプログラムとが記録された第1記録デバイス8、9と、を有する。

【0058】

ステップS70において、ユーザは、クライアント端末5にコンピュータプログラムを実行するための命令を与える。これに応答して、クライアント端末5は、適切なコンピュータプログラムの制御下で動作し、第1記録デバイス8、9から機器IDを復号化し、及び第2記録デバイス（ROM）から機器IDを復号化する（ステップS72）。ステップS74において、これらの機器IDが互いに一致するかどうか決定される。それらが一致しない場合、処理フローは、図15～18を参照して以下詳細を記載する再登録処理へと進む。これらの機器IDが一致した場合、処理フローは、クライアント端末5の復号化デバイスが機器ID（好適にROMに含まれる）を使用して、暗号化された仮想IDを復号化するステップS76へ進む。ステップS78では、クライアント端末5の復号化デバイスは、ステップS76で入手された仮想IDを使用して、クライアント暗号化コンピュータプログラムを復号化する。この時点で、クライアント端末5はRAMに存在するコンピュータプログラムを実行する。

10

【0059】

本実施形態の利点としては、クライアントで暗号化されたコンピュータプログラムは、クライアント暗号化コンピュータプログラムを暗号化するために使用される仮想IDに関連するクライアント端末5を使用することによってのみ復号化されることが挙げられる。従って、クライアントで暗号化されたコンピュータプログラムの不正なコピーが正規ではないエンドユーザに提供された場合、その正規ではないエンドユーザがコンピュータプログラムを実行しようとしても、暗号化されたコンピュータプログラムを復号化することはできない。更に第1記録デバイス8、9が正規ではないエンドユーザ（例えば、記録媒体8、9が他のクライアント端末5に接続されている場合）に提供された場合、暗号化された仮想IDは、ROMに記録されている機器IDが第1記録デバイス8、9に含まれている機器IDと一致しない限り復号化されない。従って、クライアントで暗号化されたコンピュータプログラムを復号化することは不可能である。コンピュータプログラムのセキュアな配信に対するこの斬新なアプローチによって、コンピュータプログラムの不正なコピーを使用不可にしたり、及び特定のクライアント端末5のみがコンピュータプログラムを実行を可能にすることが保証される。

20

【0060】

上述のように、コンピュータプログラムは、コンピュータプログラムビデオゲーム、ワードプロセッサプログラム、表計算ソフト等のようなアプリケーションプログラムであり、又はオペレーティングシステム（OS）、ブートプログラム等のシステムプログラムである。

30

【0061】

上記したように図13、14を参照すると、ユーザがクライアント暗号化コンピュータプログラムの実行の意志を示した場合、第1記録デバイス8、9に含まれる機器IDとクライアント端末5の第2記録デバイス（ROM）に含まれる機器IDとが一致するかどうかステップS74で判定される。これらの機器IDが一致しない場合、処理フローは図15を参照して記載される再登録処理へと分岐する。

【0062】

クライアント端末5が、別のクライアント端末機器5の記録デバイス8、9と接続されるという不適切な変更がなされた場合、これらの機器IDは一致しない。一方、クライアント端末5が修理され、この修理に伴って第2記録デバイスROMに記録された機器IDが変更された場合も、これらの機器IDは互いに異なるものとなる。また更に、例えばユーザが何らかの理由でクライアント端末を新たなクライアント端末5と入れ替え、その一方で第1記録デバイス8、9には、ひとつ又は二つ以上のクライアントで暗号化されたコンピュータプログラムが記録されていることから、この第1記録デバイスをそのまま交換しなかったという場合でも、これらの機器IDは一致しなくなる。いずれの場合においても、本発明によれば再登録（又は更新登録）処理がなされる。これらの機器IDが互いに一致しない場合、たとえコンピュータプログラムを正規に入手していたとしても、第1記

40

50

録デバイス8, 9に保存されているコンピュータプログラムを実行することはできない。当然、ユーザはコンピュータプログラムを（もとの暗号ソースの形式で容易に入手可能だとしても）再インストール可能であるが、しかしながら、本発明によれば、この相当困難な処理を回避することができる。

【0063】

図15の主記録デバイスの詳細を記載する前に、第1記録デバイス8, 9に記録されたコンピュータプログラムやデータに対しては、前述の図面とはその名称の付け方が多少異なっていることに留意されたい。詳細には、第1記録デバイス8, 9は、パーソナライズされたシステムプログラム、パーソナライズされたアプリケーションプログラム、及びパーソナライズ情報とを含む。パーソナライズされたシステムプログラム及びパーソナライズされたアプリケーションプログラムは、上記したようにクライアントで暗号化されたプログラムと関連する。パーソナライズ情報は、機器IDと、配信IDと、暗号化された仮想IDのうちの一つ以上に関連する。

【0064】

図15を更に詳細に説明すると、旧クライアント端末又は故障したクライアント端末5Fがサポートセンター11に送られる処理が示され、このサポートセンター11で修理又は交換が行われて、新たなクライアント端末装置5Nがユーザに提供される。好適には、サポートセンター11は、新たなクライアント端末5Nから配信サーバ3に新たな機器IDを伝送するのみならず、故障した端末装置5Fからの旧機器IDをも配信サーバ3に伝送する。

【0065】

更に図16と図17を参照すると、好適には、配信サーバ3は故障した端末5Fから旧機器IDを、新たなクライアント端末5Nからの新たな機器IDとともに受信する。その後、配信サーバ3はパーソナライズデータベース7にアクセスし、旧クライアント端末5Nの機器ID、例えば機器ID K6789を検出する。この検出は、関連付けられた仮想ID B9012（及び媒体ID M2468も）を入手するために行われる。次にパーソナライズデータベース7に記録された機器IDから、新たなクライアント端末装置5Nの新たな機器ID K1143が索出される。次に旧機器ID K6789と関連付けられた仮想ID B9012が、新たな機器ID K1143（及び旧媒体IDにも）関連付けられる。この処理段階で、配信サーバ3は、ユーザがユーザ自身の登録情報を更新できる状態となる。

【0066】

前述のように、ユーザが、第1記録デバイス8, 9に存在するコンピュータプログラムの実行をクライアント端末装置5Nに命令すると、第1記録デバイス8, 9及び第2記録デバイス（ROM）に記録された各機器IDが一致するかどうか判定される（ステップS70-S74, 図14参照）。更に、図18に示されるように、両機器IDが一致しないと判定されると（ステップS74, 図14参照）、ユーザに対して、好適には、配信サーバ3に対して登録情報の更新を行うことが促される（ステップS51）。ステップS52において、ユーザがクライアント端末5に登録更新処理実行の指示をしたかどうか判定される。そのような指示が受信されない場合、好適にはS51に戻り、ユーザは再度登録情報を更新するように促される。ユーザが登録情報をアップデートするための指示を出した後に、処理は好適にはステップS52からステップS53へと進み、新たなクライアント端末装置5Nの第2記録デバイス（ROM）に含まれる機器IDがネットワーク6を通じて配信サーバ3に伝送される（ネットワークインターフェースによる）。S54において、管理サーバは、パーソナライズデータベース7にアクセスすることでこの情報を確認する。その後、旧仮想ID（本来旧クライアント端末5Fに関連付けられていた仮想ID）は新たな機器ID（K1143）を使用して暗号化され、ネットワーク6を通じて（例えば配信サーバ3のネットワークインターフェースを通じて）新たなクライアント端末5Nに伝送される。

【0067】

ステップS56において、新たなクライアント端末5Nは、新たな暗号化された仮想ID（パーソナライジングデータベース情報）を受信し、そして好適には、暗号化された旧仮想IDを入れ替えるという手法で、第1記録デバイス8、9に記録する。これで登録アップデート処理は完了する。

【0068】

本実施形態では、元々は故障したクライアント端末5Fに使用されていたクライアント暗号化コンピュータプログラムを、新たな暗号化された仮想IDを用いて復号化することができるという利点が得られる。何故なら、新たな暗号化された仮想IDは、旧暗号化された仮想IDと同じ仮想IDを含むからである。換言すると、旧暗号化された仮想IDと新たに暗号化された仮想IDとは、仮想IDを暗号化するために使用される機器IDのみが異なるに過ぎない。ユーザが新たなクライアント端末5N上でクライアント暗号化コンピュータプログラムを実行するために、図13、図14を参照した上記の処理ステップが実行される。

【0069】

図19に、本発明の他の1つ以上の実施例を示す処理フローチャートを示す。本発明のこの実施例は、レンタルプログラムの配信元からの安全なプログラムの伝送を目的とする。レンタルプログラムの配信元はサードパーティサーバ1、管理サーバ4、配信サーバ3、又は他のサーバ（示されていない）としてよい。クライアント端末5のユーザが、プログラムコンテンツのレンタルを望む場合、ユーザは、好適には、レンタルシステムの会員になることが要求される。これに関してステップS70では、例えば、クライアント端末5のアクティベート機構を通じて、このレンタルシステムの会員になる意思表示を行う。例として、クライアント端末5は、入会処理を容易にする適切なコンピュータプログラムを含み、このコンピュータプログラムを実行する。

【0070】

ステップS72において、クライアント端末5は、好適にネットワーク6を通じて管理サーバ4と通信リンクを確立する。ステップS74において、クライアント端末5によるレンタルシステムの会員になるという要求がなされ、好適にはクライアント端末5がネットワーク6を通じて機器IDを管理サーバ4に伝送する。これに応答して管理サーバ4は、実質的にクライアント端末5に固有である電子会員証明書を生成する。管理サーバ4は、例えば本発明の上述の実施例のデータベース関連技術を使用して電子会員証明書とクライアント端末5の機器IDとを関連付ける。ステップS80において、管理サーバ4は、好適にネットワーク6を通じてクライアント端末5に電子会員証明書を伝送する。後述するように、電子会員証明書はレンタル処理において使用される。

【0071】

クライアント端末5が、レンタルシステムの会員になった後、ユーザは、好適にはアプリケーションプログラム及びシステムプログラムのようなプログラムをレンタルする許可が提供される。好適な実施例では、プログラムコンテンツはビデオコンピュータプログラムである。図20に示されるように、クライアント端末5で実行されているコンピュータソフトウェアによって、好適には、ユーザがコンピュータプログラムをレンタルする意思表示を行うことができる。このユーザからの指示に応答して（ステップS82）、クライアント端末5が、配信元との間に通信リンクを確立し、この通信リンクを通じて、ユーザによるレンタル要求が配信装置に配信される。（ステップS84）。ステップS86において、配信装置では、例えば、クライアント端末5の機器IDを分析することにより、又は電子会員証明書を解析することにより、好適にクライアント端末5を識別する。これは、クライアント端末5が、機器ID及び／又は電子会員証明書を配信装置に提供すること、及び配信装置がこの情報が認証されるデータベースへのアクセスを有すること、を要求することにより達成される。

【0072】

クライアント端末5が識別されたと仮定して、配信装置は、好適にネットワーク6を通じてクライアント端末5にレンタル可能なタイトルのリスト又はメニューを提供する（ステ

ップS88)。クライアント端末5に実行されているコンピュータソフトウェアは、ユーザがタイトルを選択し、レンタル期間を指定できるようにユーザにタイトルのリスト又はメニューを好適に表示するためのものである(ステップS90)。ユーザの選択結果及び指定されたレンタル期間は、ネットワーク6を通じて配信装置へ好適に伝送される。

【0073】

ステップS92において、配信装置は、好適には、クライアント端末5が指定した期間分のコンピュータプログラムのレンタル料に相当する送金を行うことを要求する。これは、公知の技術のいずれをも使用して、例えばクレジットカード番号、需要者の預金口座番号、請求決済等を伝送することにより、達成される。送金が行われた後に、好適には配信装置は指定されたタイトルのレンタル期間に関する送金が為されたことを示す電子決済チケットを生成する(ステップS94)。ステップS96において、配信装置はネットワーク6を通じて好適に電子決済チケットをクライアント端末5に伝送する。

【0074】

本発明によれば、電子決済チケットは、ユーザ(又はクライアント端末5)に対して、配信元への送金がされると、所定のレベルのレンタル権を好適にユーザに提供する。例えば、これらのレンタル権では、コンピュータプログラムのタイトル、レンタル期間、送金代価等が特定されている。加えて電子決済チケットは、コンピュータプログラムの復号化が可能である復号化鍵のように、付加情報を含むようにできる。電子決済チケットが復号化鍵を含むことは必須ではない。実際、このように復号化鍵を電子決済チケットに含めることは、単に一例に過ぎない。電子決済チケットは、例えば、復号化鍵を、暗号化された状態で含むようにしてもよい。この暗号化は、機器IDを使用して暗号化することにより、又は電子会員証明書(仮想ID等)の一部の情報を使用することにより行うことができる。いずれにしても、処理のこの時点において、ユーザは、所定のレベルのレンタル権を好適に受信するが、コンピュータプログラム又は暗号化されたコンピュータプログラムまだ受信していない。

【0075】

処理のこの段階でクライアント端末5は、機器IDと、電子会員証明書と、あるタイトルの一定期間レンタル分の送金が行われたことを示す電子決済チケットを有する。図21に示されるように、クライアント端末5は、ネットワーク6を通じて好適に管理サーバ4と通信リンクを構築する(ステップS98)。ステップS100において、管理サーバ4は、機器ID又は電子会員証明書によりクライアント端末5を識別する。これは、予め付与された電子会員証明書とクライアント端末装置5の機器IDとの関連付けが記録された、パーソナライジングデータベース6のような適切なデータベースにアクセスすることにより達成される。ステップS102において、クライアント端末5は、ネットワーク6を通じて管理サーバ4に好適に電子決済チケットを送信する。これに応答して、管理サーバ4は、電子レンタルチケットを好適に生成し(ステップS104)、ネットワーク6を通じてクライアント端末5に電子レンタルチケットを伝送する(ステップS106)。

【0076】

本発明によれば、電子レンタルチケットは、電子決済チケットで提供されるレンタル権と同様の又はそれ以上のレベルのレンタル権をユーザ(又はクライアント端末装置5)に好適に提供する。例えば、電子レンタルチケットは(電子決済チケットに復号化鍵が含まれていない場合)、コンピュータプログラムタイトル、レンタル期間、送金代価を特定し、及び暗号化されたコンピュータプログラムを復号化することが可能である復号化鍵のような付加情報を含む。電子レンタルチケットが復号化鍵を含むことは必須ではなく、実際このように復号化鍵が含まれる例は、単に例示的なものにすぎない。また、電子レンタルチケットは、復号化鍵を暗号化された形態で含むようにしてもよい。例えば、この暗号化を、機器IDを使用して又は電子会員証明書(仮想ID等)の一部である他の情報を使用して行ってもよい。いずれにせよ、処理のこの時点ではユーザは所定レベルのレンタル権を受信するが、コンピュータプログラム又はコンピュータプログラムの暗号化されたバージョンをまだ受信していない。

【0077】

図22に示されるように、クライアント端末5は、好適には、ネットワーク6を通じて配信装置と通信リンクを構築する(ステップS108)。これに応答して、配信装置では、上記のように例えば機器ID又は電子会員証明書を分析することで、クライアント端末5を識別する(ステップS110)。次に、クライアント端末5は、ネットワーク6を通じて配信装置に電子決済チケット(又は電子決済チケットの少なくとも一部)を送送する(ステップS112)。好適には、これは配信装置に対して、クライアント端末5がレンタルに関するすべての必要な前ステップを完了し、コンピュータプログラムの暗号化されたバージョンを受信することが認可されたことを示す(ステップS114)。処理のこの時点でクライアント端末5は機器ID、電子会員証明書(存在する場合には仮想IDも含む)、電子決済チケット、電子レンタルチケット、暗号化された復号化鍵及び暗号化コンピュータプログラムを好適に有する。

10

【0078】

本発明によれば、ユーザは本発明の実施例に関連して上記処理を使用して、コンピュータプログラムをロード、インストール及び実行することが考えられる。本発明のレンタルシステムの実施例は、ネットワーク6を通じて、クライアント端末5の台数にかかわらずレンタルプログラムの安全な配信が可能となるという点で有利である。

【0079】

以上、本発明を特定の実施形態により説明したが、実施形態は本発明の原理及び応用に単に例示的に説明したに過ぎない。従って、請求項に規定した本発明の精神及び範囲から逸脱することなく、これらの例示的な実施形態にたいして種々の変形をおこなうことができる。

20

【図面の簡単な説明】

【0080】

【図1】本発明の1つ以上の形態に係る1人以上のユーザに対してのプログラムコンテンツ配布システムの模式図である。

【図2】図1に示すシステムの一部において実行される処理ステップを示す概念的ブロックとそのフローの説明図。

【図3】図1に示すシステムの一部において実行される処理ステップを示す概念的ブロックとそのフローの説明図。

30

【図4】図3に示された本発明に従って実行される処理ステップを示すフローチャート。

【図5】例えば、図1に示す管理サーバとクライアント端末により実行される処理ステップを示す概念的ブロック図とフローチャート。

【図6】図5に示す装置により実行されるさらなる処理ステップを示すフローチャート。

【図7】図1に示すシステムにより実行される処理ステップを示す概念的ブロック図。

【図8】図1に示すシステムにより実行される所定の処理ステップを示す概念的ブロック図とフローチャート。

【図9】図8に示す装置により実行されるさらなる処理ステップを示すフローチャート。

【図10】本発明に係る所定のデータベースの内容を示す模式図。

【図11】例えば、図1に示すクライアント端末により実行される、1つ以上の更なる処理手段を示すさらなる概念的ブロック図とフロー説明図。

40

【図12】図1により実行される更なる処理ステップを示すフローチャート。

【図13】本発明に係るクライアント端末により実行される1つ以上のさらなる処理ステップを示す概念的ブロック図とフロー説明図。

【図14】図13に示すさらなる詳細を鑑みた処理ステップを示すフローチャート。

【図15】本発明のさらなる様態を示す概念的ブロック図とフローチャート。

【図16】本発明の1つ以上の様態に従った所定のデータベースの内容を示す模式図。

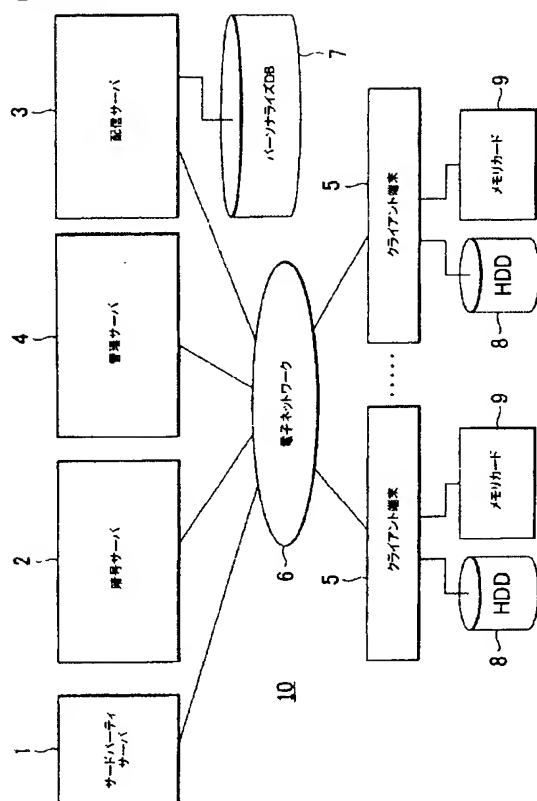
【図17】図16に示すデータベースの内容の更なる機能を示す模式図。

【図18】図15に示すベース内容の更なる詳細を鑑みた処理ステップを示すフローチャート。

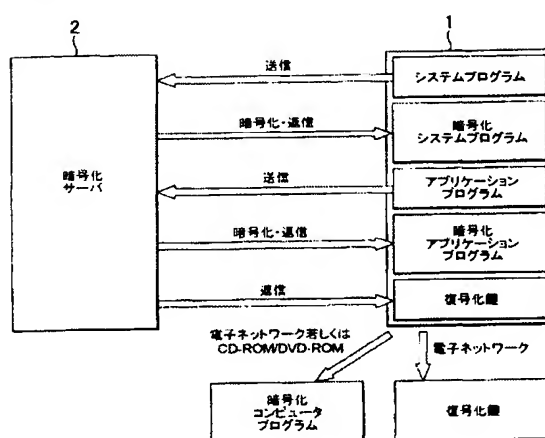
50

- 【図19】 本発明の1つ以上の形態を示すフローチャート。
 【図20】 図19に係る本発明の更なる処理ステップを示すフローチャート。
 【図21】 図20に係る本発明の更なる処理ステップを示すフローチャート。
 【図22】 図21に係る本発明の更なる処理ステップを示すフローチャート。

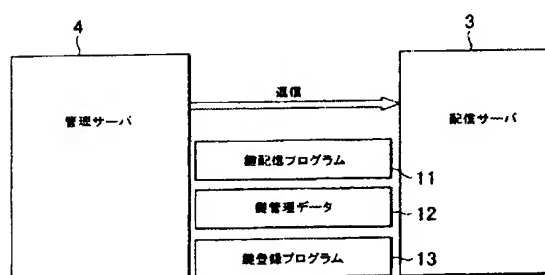
【図1】



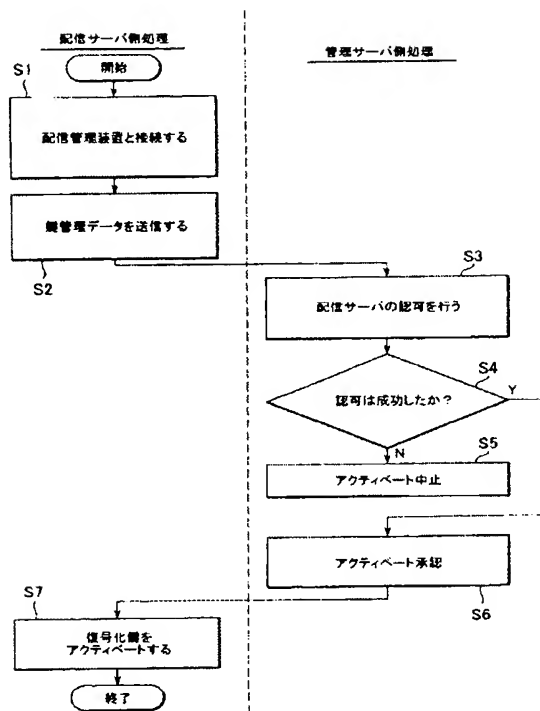
【図2】



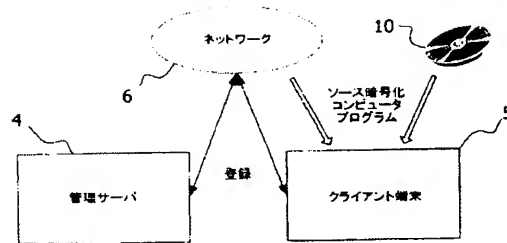
【図3】



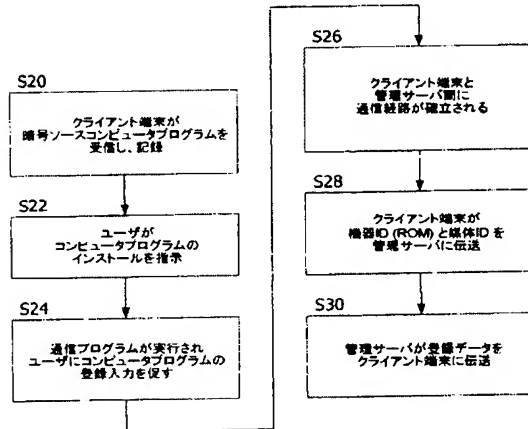
【図4】



【図5】



【図6】

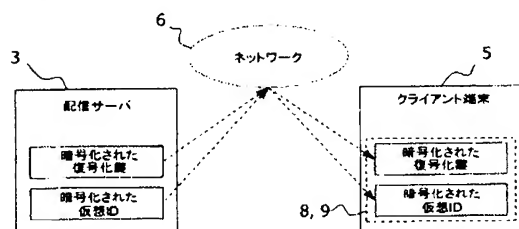


【図7】

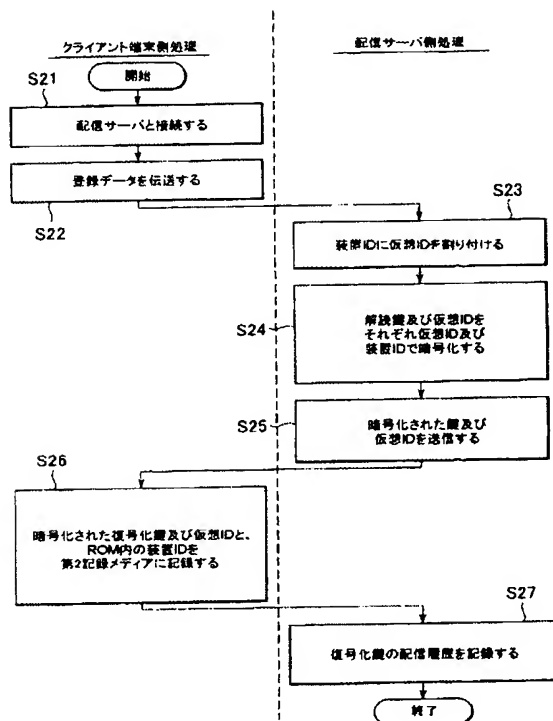
7A

デバイスID	配信元ID
K1234	D3456
K2345	D1278
K6789	--
K0987	--

【図8】



【図9】

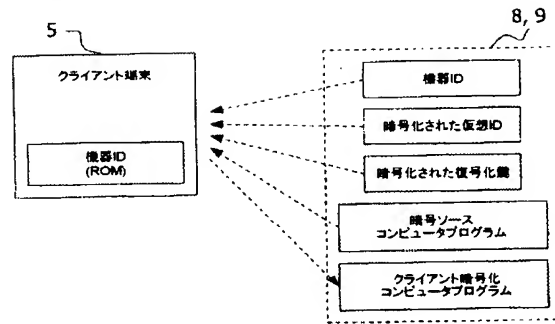


【図10】

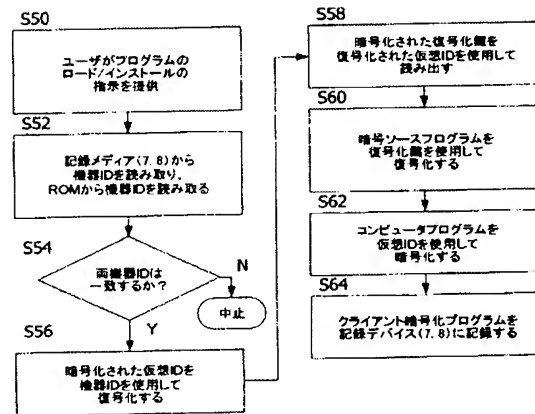
↙ Z

機器ID	仮想ID
K1234	—
K2345	B5678
K6789	B9012
K0987	—
⋮	⋮

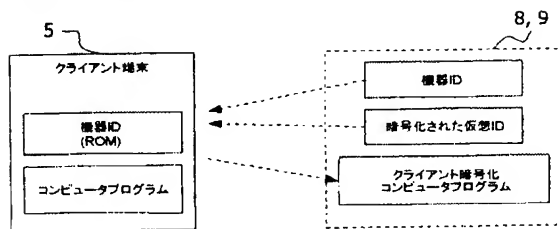
【図11】



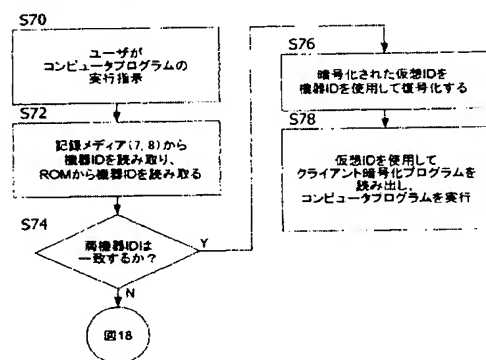
【図12】



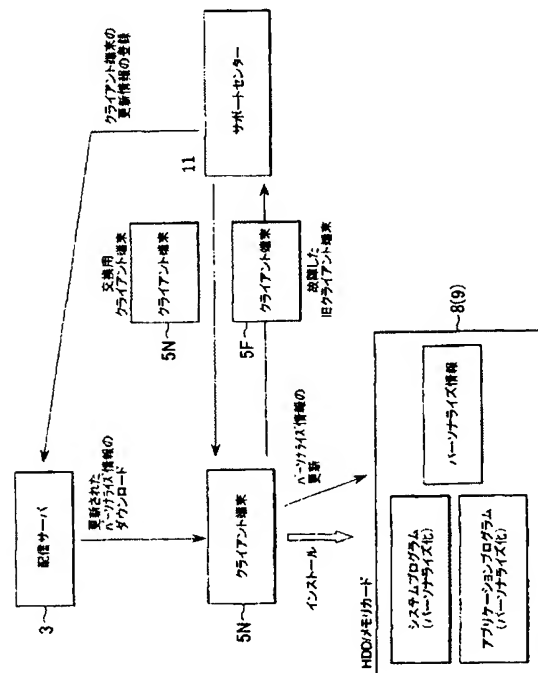
【図13】



【図14】



【図15】



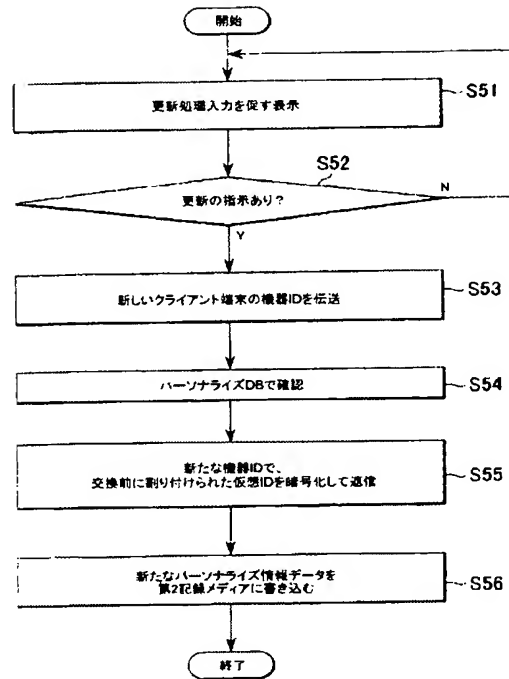
【図16】

機器ID	仮想ID
K1234	—
K2345	B5678
K6789	B9012
K0987	—
⋮	⋮

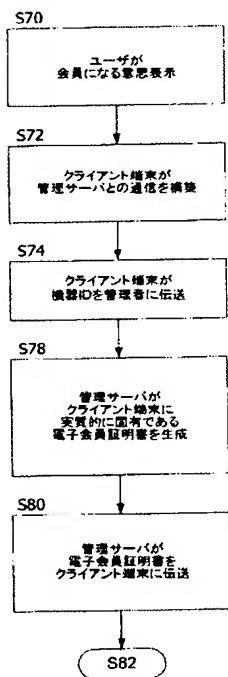
【図17】

機器ID	仮想ID
K1234	—
K2345	B5678
K1143	B9012
K0987	—
⋮	⋮

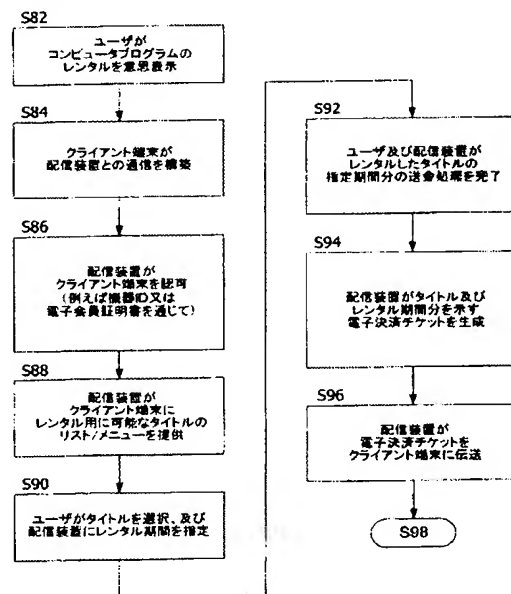
【図18】



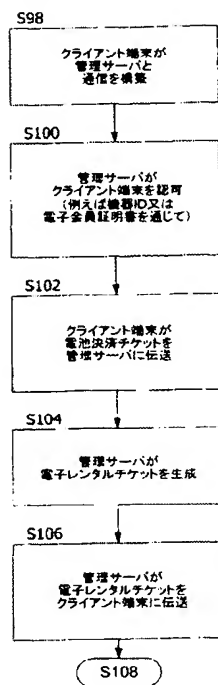
【図19】



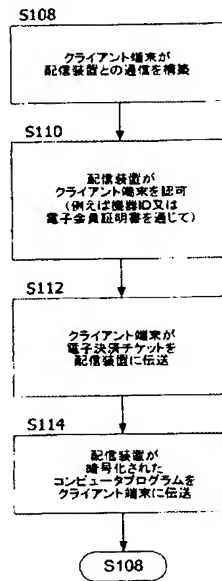
【図20】



【図21】



【図22】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/12738

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L 9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L 9/08, G06F 9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
 Japanese Utility Model Gazette 1926-1996, Japanese Publication of Unexamined Utility Model Applications 1971-2003, Japanese Registered Utility Model Gazette 1994-2003, Japanese Gazette Containing the Utility Model 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-242604 A (FUJITSU K.K.) 2000.09.08 page 4, column 5, line 46 -page 5, column 8, line 1 figures 1-2 (No families)	1-38
A	JP 11-275516 A (HITACHI SEISAKUSHYO K.K.) 1999.09.08 page 8, column 13, line 30 -page 8, column 14, line 5 figure 6 (No families)	1-38

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

14.03.03

Date of mailing of the international search report

25.03.03

Name and mailing address of the ISA/JP

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan

Authorized officer

Hiromasa Nakazato

Telephone No. +81-3-3581-1101 Ext. 3599



SM

9364

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/12738

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/56068 A1 (THOMSON LICENSING S.A.) 2000.09.21 See whole document & AU 200036291 A & CN 1343420 A & EP 1169856 A1 & JP 2002-539724 A & KR 2001105384 A & MX 2001009286 A	1-38

フロントページの続き

- (72)発明者 岡田 豊史
日本国東京都港区南青山2-6-21 株式会社ソニー・コンピュータエンタテインメント内
- (72)発明者 木本 陽介
日本国東京都港区南青山2-6-21 株式会社ソニー・コンピュータエンタテインメント内
- (72)発明者 金江 和広
日本国東京都港区南青山2-6-21 株式会社ソニー・コンピュータエンタテインメント内
- (72)発明者 小巻 賢二郎
日本国東京都港区南青山2-6-21 株式会社ソニー・コンピュータエンタテインメント内
- Fターム(参考) 5J104 EA17 EA18 EA26 PA07